REMARKS

In the Office Action mailed September 30, 2004, the Examiner noted that claims 52-110 were pending and rejected claims 52-110. Claims 52-110 remain pending for reconsideration which is requested. The Examiner's rejections are traversed below.

On page 2 of the Office Action, the Examiner rejected all claims under 35 U.S.C. § 102 as anticipated by Arnold.

In the Action the Examiner provided specific comments about claims 52, 53 and 54 but not about claims 55-110. In particular, the Examiner alleged that the "a saving unit saving a detected virus-infected file into a specific area within said storage device" of claim 52 is shown by Arnold at col. 19, lines 58-68, col. 20, lines 1-11 and col. 29, lines 26-40. These portions of Arnold particularly state:

> The kill signal may take a variety of forms and provide as little or as much information as is appropriate or practical. For example, in one embodiment the infected computer simply sends an "I'm infected" signal (one bit of information) to its neighbor(s) whenever it enters Step B (Scan for Known Viruses), thereby inducing all of the neighbors to also enter Step B themselves. In another embodiment, the infected computer sends an "I'm infected" signal after it has cleaned itself up (completed Step B successfully), and also sends the name of the virus (if it was previously known) and its signature(s), whether the virus was previously known or not. The signature(s) may have been determined in Step E. In a further embodiment, the infected computer sends an "I'm infected" signal when it enters Step C, i.e., after it fails to identify the anomaly as a known virus, thereby inducing its neighbors to enter Steps B and C. Other strategies may also be used, other than those specifically detailed above. In all cases, the end result is that other computers on the network are alerted to the presence of an anomaly, which may be a known or an unknown virus, within the network.

(See Arnold, col. 19, line 58-col. 11, line 11)

> A feature of this invention is the taking of remedial action in the event that a known or unknown signature of an undesirable software entity is identified or extracted. Remedial action includes killing or removing the undesirable software entity, and also possibly informing neighboring data processors of the existence and signature of the entity. Possible methods for removing the undesirable software entity include, but are are not limited to, (a) replacing an infected file with a stored, secured, uninfected version of the file; (b) repair mechanisms designed for specific known types of undesirable software entities; and (c) heuristic repair mechanisms which are designed for classes of undesirable software entities.

(See Arnold, col. 29, lines 26-40)

As can be seen from the above text and as acknowledged by the Examiner, this portion discusses "... specifically wherein replacing an infected file with a stored, secured, uninfected version of the file ..." (see Action page 3).

In contrast, the present invention of claim 52 does not kill or destroy and replace the file with an uninfected file but rather saves the file ("saving a detected virus-infected file into a specific area within said storage device" – claim 52). Saving the file is very different from destroying the file. By saving the file, the file can be analyzed or examined, something not possible in Arnold. The present invention of claim 52 is very different from Arnold. Similar language to claim 52 also appears in independent claims 57, 62 and 110. Independent claims 67, 75, 88, 94, 101, 107 and 108 provide a similar benefit by emphasizing that the infected file is quarantined. Arnold does not discuss or suggest quarantining a file. Independent claims 72, 79, 84, 85, 92, 97, 98 and 105 emphasize encrypting an infected file. This is certainly not killing the file as in Arnold. Arnold does not discuss or suggest encrypting a file. Independent claim 109 emphasizes isolating an infected file from other files. This is also certainly not killing the file as in Arnold. Arnold does not discuss or suggest isolating a file.

It is submitted that the present claimed invention of the independent claims patentably distinguishes over Arnold and withdrawal of the rejection is requested.

The dependent claims depend from the above-discussed independent claims and are patentable over the prior art for the reasons discussed above. The dependent claims also recite additional features not taught or suggested by the prior art. For example, claim 70, which is dependent from a claim that calls for quarantining the file, emphasizes that the quarantined file is encrypted. As discussed above Arnold does not discuss or suggest encrypting a file much less teach or suggest encrypting a quarantined file. It is submitted that the dependent claims are independently patentable over the prior art.

It is submitted that the claims are not taught, disclosed or suggested by the prior art. The claims are therefore in a condition suitable for allowance. An early Notice of Allowance is requested.

If any further fees, other than and except for the issue fee, are necessary with respect to this paper, the U.S.P.T.O. is requested to obtain the same from deposit account number 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

Date: 3/30/05

By: _____
J. Randall Beckers
Registration No. 30,358

1201 New York Avenue, NW, Suite 700
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501